#4

Europäisches Patentamt | European Patent Office | Office européen des brevets

JC530 U.S. PTO
09/365211
07/30/99

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. | Patent application No. | Demande de brevet n°

98890222.7

CERTIFIED COPY OF PRIORITY DOCUMENT

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

Arlette Fiedler

A. Fiedler

DEN HAAG, DEN
THE HAGUE,
LA HAYE, LE 21/01/99

EPA/EPO/OEB Form 1014 - 02.91

Europäisches Patentamt
European Patent Office
Office européen des brevets

Blatt 2 der Bescheinigung
Sheet 2 of the certificate
Page 2 de l'attestation

Anmeldung Nr.:
Application no.:
Demande n°: 98890222.7

Anmeldetag:
Date of filing:
Date de dépôt: 31/07/98

Anmelder:
Applicant(s):
Demandeur(s):
Koninklijke Philips Electronics N.V.
5621 BA Eindhoven
NETHERLANDS

Bezeichnung der Erfindung:
Title of the invention:
Titre de l'invention:
Datenverarbeitungseinrichtung mit einen Kennwert nutzenden Datenverarbeitungsmitteln und mit Mitteln zum Abwehren von Analysemethoden zur Ermittlung des Kennwertes

In Anspruch genommene Priorität(en) / Priority(ies) claimed / Priorité(s) revendiquée(s)

Staat: State: Pays:	Tag: Date: Date:	Aktenzeichen: File no. Numéro de dépôt:

Internationale Patentklassifikation:
International Patent classification:
Classification internationale des brevets:
/

Am Anmeldetag benannte Vertragstaaten:
Contracting states designated at date of filing: AT/BE/CH/CY/DE/DK/ES/FI/FR/GB/GR/IE/IT/LI/LU/MC/NL/PT/SE
Etats contractants désignés lors du dépôt:

Bemerkungen:
Remarks:
Remarques:

Datenverarbeitungseinrichtung mit einen Kennwert nutzenden Datenverarbeitungsmitteln und mit Mitteln zum Abwehren von Analysemethoden zur Ermittlung des Kennwertes

Die Erfindung bezieht sich auf eine Datenverarbeitungseinrichtung mit einer Schaltung, die aus verschiedenen Schaltungsteilen besteht, die über eine Leitungskonfiguration mit einer Versorgungsspannung versorgbar sind, und die Datenverarbeitungsmittel enthält, die einen solchen mit der Versorgungsspannung versorgbaren Schaltungsteil bilden und die zum Verarbeiten von Daten unter Verwendung eines Kennwertes geeignet sind, und die Ablaufsteuermittel enthält, die auch einen solchen mit der Versorgungsspannung versorgbaren Schaltungsteil bilden und die zum Abarbeiten eines Algorithmus zum Steuern der Datenverarbeitungsmittel entsprechend diesem Algorithmus ausgebildet sind, welcher Algorithmus eine bestimmte Anzahl N von Teilalgorithmen umfaßt, in denen identische Aufeinanderfolgen von Algorithmusschritten enthalten sind und die bei jedem Abarbeiten des Algorithmus in einer bestimmten Reihenfolge abarbeitbar sind, und bei der - bei einem Verarbeiten von Daten mit den Datenverarbeitungsmitteln unter der dem Algorithmus entsprechenden Steuerung mit Hilfe der Ablaufsteuermittel - als Folge der Datenverarbeitung im Bereich der Leitungskonfiguration ein Stromspitzenmuster auftritt, wobei die Musterkonfiguration des Stromspitzenmusters von den Algorithmusschritten und von den verarbeiteten Daten und von dem Kennwert abhängig ist.

Die Erfindung bezieht sich weiters auf eine Schaltung für eine Datenverarbeitungseinrichtung, die aus verschiedenen Schaltungsteilen besteht, die über eine Leitungskonfiguration mit einer Versorgungsspannung versorgbar sind, und die Datenverarbeitungsmittel enthält, die einen solchen mit der Versorgungsspannung versorgbaren Schaltungsteil bilden und die zum Verarbeiten von Daten unter Verwendung eines Kennwertes geeignet sind, und die Ablaufsteuermittel enthält, die auch einen solchen mit der Versorgungsspannung versorgbaren Schaltungsteil bilden und die zum Abarbeiten eines Algorithmus zum Steuern der Datenverarbeitungsmittel entsprechend diesem Algorithmus ausgebildet sind, welcher Algorithmus eine bestimmte Anzahl N von Teilalgorithmen umfaßt, in denen identische Aufeinanderfolgen von Algorithmusschritten

enthalten sind und die bei jedem Abarbeiten des Algorithmus in einer bestimmten Reihenfolge abarbeitbar sind, und bei der - bei einem Verarbeiten von Daten mit den Datenverarbeitungsmitteln unter der dem Algorithmus entsprechenden Steuerung mit Hilfe der Ablaufsteuermittel - als Folge der Datenverarbeitung im Bereich der Leitungskonfiguration ein Stromspitzenmuster auftritt, wobei die Musterkonfiguration des Stromspitzenmusters von den Algorithmusschritten und von den verarbeiteten Daten und von dem Kennwert abhängig ist.

Eine Datenverarbeitungseinrichtung entsprechend der eingangs im ersten Absatz angeführten Gattung und eine Schaltung entsprechend der eingangs im zweiten Absatz angeführten Gattung sind bekannt, und zwar von in vielen Ausführungsvarianten verwendeten kontaktbehafteten Chipkarten, in denen ein integrierter Baustein enthalten ist, der von der Anmelderin entwickelt und in den Handel gebracht wurde. Bei der bekannten Datenverarbeitungseinrichtung, also bei der bekannten kontaktbehafteten Chipkarte, und bei der bekannten Schaltung, also bei dem in einer solchen bekannten kontaktbehafteten Chipkarte enthaltenen bekannten integrierten Baustein, sind die Datenverarbeitungsmittel durch Verschlüsselungsmittel gebildet, die entsprechend dem „Data Encryption Standard" (DES) eine Verschlüsselung von ihnen zugeführten Daten unter Verwendung eines ihnen ebenso zugeführten Kennwertes, nämlich eines geheimen Schlüssels, durchführen. Bei einer solchen Verschlüsselung werden insgesamt N = 8 sogenannte SBOX-Einheiten abgearbeitet, wobei mit Hilfe von jeder SBOX-Einheit eine Berechnung eines SBOX-Ergebnisses durchgeführt wird. Die Abarbeitung aller acht SBOX-Einheiten erfolgt im Rahmen eines einen Algorithmus bildenden Programmes, von dem jeder Programmblock, der einen Teilalgorithmus bildet, einer SBOX-Einheit entspricht. Jeder Programmblock, der einer SBOX-Einheit entspricht, enthält eine für die betreffende SBOX-Einheit charakteristische Tabelle, in der Einträge enthalten sind, wobei sich die Einträge aller SBOX-Einheiten voneinander unterscheiden. Mit Hilfe der in einer SBOX-Einheit enthaltenen Tabelle bzw. den Einträgen in dieser Tabelle werden zu den einer SBOX-Einheit zugeführten Eingangsdaten zugehörige Ausgangsdaten ermittelt. Dieses Ermitteln von zu Eingangsdaten zugehörigen Ausgangsdaten erfolgt aber bei allen acht SBOX-Einheiten unter Ausnützung desselben Algorithmus zur Zuordnung zwischen

Eingangsdaten und Ausgangsdaten, was mit anderen Worten heißt, daß in allen je eine SBOX-Einheit repräsentierenden und einen Teilalgorithmus bildenden N Programmblöcken identische Aufeinanderfolgen von Programmbefehlen als Algorithmusschritte enthalten sind. Bei der bekannten Datenverarbeitungseinrichtung bzw. bei der bekannten Schaltung ist der Sachverhalt gegeben, daß bei jedem Abarbeiten des Programmes die N Programmblöcke in stets derselben Reihenfolge abgearbeitet werden.

Beim Durchführen eines Verschlüsselungsvorganges tritt im Bereich der Leitungskonfiguration ein Stromspitzenmuster auf, das abhängig von den Programmbefehlen ist und das abhängig von den Daten ist, die in den Verschlüsselungsmitteln verarbeitet werden, und das abhängig von dem in den Verschlüsselungsmitteln verwendeten Kennwert ist, also von dem geheimen Schlüssel für diese Verschlüsselungsmittel. Bei der bekannten Datenverarbeitungseinrichtung bzw. bei der bekannten Schaltung besteht das Problem, daß die jeweils verursachten Stromspitzenmuster auch in Bereichen der Schaltung bzw. in Bereichen der Datenverarbeitungseinrichtung auftreten, die von außerhalb abfragbar sind. Dieses Auftreten der jeweils verursachten Stromspitzenmuster an den erwähnten Bereichen kann beispielsweise in der Weise ausgenützt werden, daß den Datenverarbeitungsmitteln zum Verarbeiten von Daten unter Verwendung eines Kennwertes bestimmte bekannte Daten beliebig oft aufeinanderfolgend zum Verarbeiten zugeführt werden und daß während des Verarbeitens dieser bekannten Daten die hierbei verursachten stets gleichen Stromspitzenmuster einer Beobachtung bzw. einer Detektion unterzogen werden, wobei mit Hilfe von zwar aufwendigen, aber bekannten und zur Verfügung stehenden Korrelationsverfahren bzw. Vergleichsverfahren unter Ausnützung der detektierten Stromspitzenmuster Rückschlüsse auf den in den Datenverarbeitungsmitteln, also den Verschlüsselungsmitteln, verwendeten Kennwert, also den geheimen Schlüssel, gezogen werden können. Selbstverständlich ist ein solches Knacken eines geheimen Schlüssels unerwünscht, weil hierdurch eine erwünschte Geheimhaltung nicht mehr mit hoher Sicherheit gewährleistet werden kann.

Die Erfindung hat sich zur Aufgabe gestellt, die vorstehend angeführten Schwierigkeiten zu vermeiden und mit einfachen Mitteln und nur einem sehr geringen

zusätzlichen Aufwand eine verbesserte Datenverarbeitungseinrichtung bzw. eine verbesserte Schaltung für eine Datenverarbeitungseinrichtung zu schaffen, die eine hohe Sicherheit im Hinblick auf das Geheimhalten eines Kennwertes gewährleisten.

Zur Lösung der vorstehend angeführten Aufgabe ist eine Datenverarbeitungseinrichtung entsprechend der eingangs im ersten Absatz angeführten Gattung gemäß der Erfindung dadurch gekennzeichnet, daß die Schaltung zusätzlich Reihenfolge-Festlegungsmittel enthält, die mit den Ablaufsteuermitteln zusammenwirken und mit denen bei jedem Abarbeiten des Algorithmus aus einer Vielzahl von möglichen Reihenfolgen für das Abarbeiten der N Teilalgorithmen eine Reihenfolge festlegbar ist.

Zur Lösung der vorstehend angeführten Aufgabe ist weiters eine Schaltung entsprechend der eingangs im zweiten Absatz angeführten Gattung gemäß der Erfindung dadurch gekennzeichnet, daß die Schaltung zusätzlich Reihenfolge-Festlegungsmittel enthält, die mit den Ablaufsteuermitteln zusammenwirken und mit denen bei jedem Abarbeiten des Algorithmus aus einer Vielzahl von möglichen Reihenfolgen für das Abarbeiten der N Teilalgorithmen eine Reihenfolge festlegbar ist.

Durch das Vorsehen der erfindungsgemäßen Maßnahmen ist auf sehr einfache und wirksame und betriebssichere Weise erreicht, daß zwar die Aufeinanderfolge aller Algorithmusschritte aus allen hintereinander abgearbeiteten Teilalgorithmen bei jedem Abarbeiten des Algorithmus stets gleich ist, daß aber die Reihenfolge für das Abarbeiten der N Teilalgorithmen eines Algorithmus bei jedem Abarbeiten des Algorithmus unterschiedlich ist, so daß die Reihenfolge des Abarbeitens der N Teilalgorithmen von außerhalb der Datenverarbeitungseinrichtung bzw. der Schaltung der Datenverarbeitungseinrichtung nicht bestimmt werden kann. Dadurch ist es auch nicht möglich, aufeinanderfolgend verursachte Stromspitzenmuster, die durch aufeinanderfolgendes Aktivieren des Algorithmus verursacht werden, untereinander zu vergleichen und für Analysemethoden mit Hilfe von Korrelationsverfahren bzw. Vergleichsverfahren zu verwenden. Auf diese Weise ist erreicht, daß ein unerwünschtes Erkennen bzw. Feststellen eines in Datenverarbeitungsmitteln verwendeten Kennwertes, wie eines geheimen Schlüssels, praktisch nicht möglich ist oder zumindest drastisch erschwert ist.

Bei einer erfindungsgemäßen Datenverarbeitung bzw. bei einer erfindungsgemäßen Schaltung haben sich die Maßnahmen gemäß der Ansprüche 2 und 3 bzw. 7 und 8 als sehr

vorteilhaft erwiesen, weil sich diese Ausbildungen durch eine besondere Einfachheit auszeichnen und mit Hilfe von in einer erfindungsgemäßen Datenverarbeitungseinrichtung bzw. einer erfindungsgemäßen Schaltung ohnehin vorhandenen Mitteln leicht realisierbar sind. Bezüglich der Reihenfolge-Auswahlmittel sei noch erwähnt, daß in diesen Reihenfolge-Auswahlmitteln vorzugsweise nur ein Teil aller möglichen Reihenfolgen für das Abarbeiten der N Algorithmen enthalten ist, daß es aber durchaus auch möglich ist, alle möglichen Reihenfolgen für das Abarbeiten von N Teilalgorithmen in den Reihenfolge-Auswahlmitteln vorzusehen.

Als besonders vorteilhaft haben sich die erfindungsgemäßen Maßnahmen bei einer Datenverarbeitungseinrichtung gemäß dem Anspruch 4 bzw. einer Schaltung gemäß dem Anspruch 9 erwiesen, weil insbesondere bei Mitteln zum Verschlüsseln und/oder Entschlüsseln von Daten ein sehr hoher Geheimhaltungsbedarf bezüglich des verwendeten Schlüssels besteht.

Eine erfindungsgemäße Datenverarbeitungseinrichtung kann beispielsweise durch einen Computer oder durch einen Personalcomputer gebildet sein, die beispielsweise zum Abarbeiten eines Verschlüsselungsprogrammes ausgebildet sind. Als besonders vorteilhaft haben sich die erfindungsgemäßen Maßnahmen bei einer erfindungsgemäßen Datenverarbeitungseinrichtung entsprechend dem Anspruch 7 bzw. bei einer Schaltung entsprechend dem Anspruch 14 erwiesen, weil in diesen Fällen die Gefahr eines Knackens eines Kennwertes besonders groß ist.

Die vorstehend angeführten Aspekte und weitere Aspekte der Erfindung gehen aus dem nachfolgend beschriebenen Ausführungsbeispiel hervor und sind anhand dieses Ausführungsbeispieles erläutert.

Die Erfindung wird im folgenden anhand von einem in den Zeichnungen dargestellten Ausführungsbeispiel weiter beschrieben, auf das die Erfindung aber nicht beschränkt ist.

Die Figur 1 zeigt auf stark schematisierte Weise in Form eines Blockschaltbildes einen im vorliegenden Zusammenhang wesentlichen Teil einer Datenverarbeitungseinrichtung und einer Schaltung für diese Datenverarbeitungseinrichtung gemäß einem Ausführungsbeispiel der Erfindung.

Die Figur 2 zeigt auf schematische Weise drei Abläufe von ein und demselben

Programm, das aus insgesamt N Programmblöcken besteht.

In der Figur 1 ist in Form eines Blockschaltbildes ein Teil einer Datenverarbeitungseinrichtung dargestellt, die im vorliegenden Fall durch einen Datenträger 1 gebildet ist, der zum kontaktlosen Kommunizieren mit einer hierfür vorgesehenen Schreib/Lese-Station ausgebildet ist, die in der Figur 1 jedoch nicht dargestellt ist.

Der Datenträger 1 enthält eine Schaltung 2, die in integrierter Technik realisiert ist. Die Schaltung 2 besteht aus verschiedenen Schaltungsteilen, auf die nachfolgend noch näher eingegangen ist. Die Schaltungsteile sind über eine Leitungskonfiguration 3 mit einer Versorgungsspannung V versorgbar, wobei es sich um eine Versorgungs-Gleichspannung handelt. Auf die Erzeugung der Versorgungsspannung V ist nachfolgend noch näher eingegangen.

Der Datenträger 1 weist Empfangs/Sende-Mittel 4 auf, die eine Übertragungsspule 5 enthalten. Die Empfangs/Sende-Mittel 4 sind an einen ersten Anschluß 6 und an einen zweiten Anschluß 7 der Schaltung 2 angeschlossen. Die Übertragungsspule 5 ist auf induktive Weise mit einer Übertragungsspule einer nicht dargestellten Schreib/Lese-Station koppelbar. Mit Hilfe der beiden Übertragungsspulen ist es möglich, sowohl ein unmoduliertes Trägersignal CS als auch ein amplitudenmoduliertes Trägersignal CSM, das entsprechend von Daten DA, die von der Schreib/Lese-Station zu dem Datenträger 1 zu übertragen sind, amplitudenmoduliert ist, als auch ein belastungsmoduliertes Trägersignal CSB, das mit Hilfe von in der Figur 1 nicht dargestellten Belastungsmodulationsmitteln des Datenträgers 1 bzw. der Schaltung 2 dieses Datenträgers 1 erzeugbar ist und mit dessen Hilfe von dem Datenträger 1 zu einer Schreib/Lese-Station zu übertragende Daten DA übertragbar sind, zwischen den beiden miteinander in Kommunikationsverbindung stehenden Partnern, also einer Schreib/Lese-Station und dem Datenträger 1, zu übertragen. Hierbei handelt es sich um seit langem bekannte Maßnahmen.

Mit Hilfe des von einer Schreib/Lese-Station zu dem Datenträger 1 übertragenen unmodulierten Trägersignals CS und mit Hilfe des von einer Schreib/Lese-Station zu dem Datenträger 1 übertragenen amplitudenmodulierten Trägersignals CSM kann in dem Datenträger 1 die Versorgungsspannung V gewonnen werden. Hierfür wird das mit den

Empfangs/Sende-Mitteln 4 empfangene unmodulierte Trägersignal CS bzw. das amplitudenmodulierte Trägersignal CSM über den ersten Anschluß 6 und eine mit dem ersten Anschluß 6 verbundene elektrisch leitende Verbindung 8 Versorgungsspannungs-Erzeugungsmitteln 9 zugeführt. Die Versorgungsspannungs-Erzeugungsmittel 9 bestehen im wesentlichen aus einer Gleichrichterstufe und einem Speicherkondensator sowie Spannungsbegrenzungsmitteln, die eine unerwünschte Überspannung verhindern. Mit den Versorgungsspannungs-Erzeugungsmitteln 9 ist die bereits vorstehend erwähnte Versorgungsspannung V erzeugbar und über einen Ausgang 10 der Versorgungsspannungs-Erzeugungsmittel 9 an die Leitungskonfiguration 3 abgebbar. Die erzeugte Versorgungsspannung V ist über die Leitungskonfiguration 3 den verschiedenen Schaltungsteilen der Schaltung 2 zuführbar. Es sei erwähnt, daß diese Leitungskonfiguration 3 auch leitende Masseverbindungen aufweist, die in der Figur 1 aber der Einfachheit halber nicht dargestellt sind.

Der Datenträger 1 bzw. die Schaltung 2 enthalten erste Datenverarbeitungsmittel 11, denen die Versorgungsspannung V an einem Versorgungseingang 12 zuführbar ist. Weiters ist den ersten Datenverarbeitungsmitteln 11 über eine Verbindung 13A auch das von den Empfangs/Sende-Mitteln 4 abgegebene amplitudenmodulierte Trägersignal CSM zuführbar. Mit den ersten Datenverarbeitungsmitteln 11 ist über eine weitere Verbindung 13B, die zu dem zweiten Anschluß 7 geführt ist, in den Empfangs/Sende-Mitteln 4 das belastungsmodulierte Trägersignal CSB erzielbar. An die ersten Datenverarbeitungsmittel 11 ist weiters eine erste BUS-Verbindung 14 angeschlossen, die zu Ablaufsteuermitteln 15 geführt ist. Die Ablaufsteuermittel 15 sind zum Abarbeiten eines ersten Algorithmus zum Steuern der ersten Datenverarbeitungsmittel 11 entsprechend diesem ersten Algorithmus ausgebildet.

Die ersten Datenverarbeitungsmittel 11 enthalten nicht dargestellte Demodulationsmittel, mit denen ein Demodulieren des zugeführten amplitudenmodulierten Trägersignals CSM durchführbar ist. Nach einem solchen Demodulieren des amplitudenmodulierten Trägersignals CSM kann erforderlichenfalls ein Dekodieren des demodulierten Signals durchgeführt werden. Gegebenenfalls können auch noch weitere Verarbeitungsvorgänge vorgenommen werden. Nach dem Durchführen sämtlicher Verarbeitungsvorgänge geben die ersten Datenverarbeitungsmittel 11 Daten DA an eine zweite BUS-Verbindung 16 ab, die zu zweiten Datenverarbeitungsmitteln 17 geführt ist.

Die zweiten Datenverarbeitungsmittel 17 sind zum Verarbeiten von Daten DA unter Verwendung eines Kennwertes CV ausgebildet. Im vorliegenden Fall sind die zweiten Datenverarbeitungsmittel 17 durch Mittel zum Verschlüsseln und/oder Entschlüsseln von Daten gebildet, wobei der zum Verschlüsseln und Entschlüsseln erforderliche geheime Schlüssel durch den zuvor erwähnten Kennwert CV gebildet ist.

Die zweiten Datenverarbeitungsmittel 17 weisen einen Versorgungseingang 18 auf, über den die zweiten Datenverarbeitungsmittel 17 mit der Versorgungsspannung V versorgbar sind. Weiters ist an die zweiten Datenverarbeitungsmittel 17 eine dritte BUS-Verbindung 19 angeschlossen, die andererseits zu den Ablaufsteuermitteln 15 geführt ist. Die Ablaufsteuermittel 15 sind auch zum Abarbeiten eines zweiten Algorithmus zum Steuern der zweiten Datenverarbeitungsmittel 17 entsprechend diesem zweiten Algorithmus ausgebildet.

Im vorliegenden Fall des Datenträgers 1 gemäß der Figur 1 sind in der Schaltung 2 Programmspeichermittel 20 vorgesehen, die mit den Ablaufsteuermitteln 15 zusammenwirken und in denen der zweite Algorithmus in Form eines Programmes P gespeichert ist. Der zweite Algorithmus, also das Programm P, umfaßt eine bestimmte Anzahl N von Teilalgorithmen, die im vorliegenden Fall durch N Programmblöcke PB1, PB2, PB3 usw. bis PBN gebildet sind. In den Teilalgorithmen, die durch die Programmblöcke PB1 bis PBN gebildet sind, sind identische Aufeinanderfolgen von Algorithmusschritten enthalten, die im vorliegenden Fall durch Programmbefehle CO1, CO2, CO3 usw. bis COR gebildet sind. Die N Teilalgorithmen, also die N Programmblöcke, sind bei jedem Abarbeiten des Algorithmus, also des Programmes P, in einer bestimmten Reihenfolge abarbeitbar, worauf nachfolgend noch näher eingegangen ist. Die Programmspeichermittel 20 sind mit den Ablaufsteuermitteln 15 über eine vierte BUS-Verbindung 21 verbunden, so daß über die vierte BUS-Verbindung 21 ein Zusammenwirken der Programmspeichermittel 20 und der Ablaufsteuermittel 15 ermöglicht ist. Die Programmspeichermittel 20 weisen einen Versorgungseingang 22 auf, über den den Programmspeichermitteln 20 die Versorgungsspannung V zuführbar ist.

Die Schaltung 2 enthält weiters Speichermittel 23, die einen Daten-Speicherteil 24 und einen Kennwert-Speicherteil 25 umfassen. Der Daten-Speicherteil 24 ist zum Speichern von Daten DA vorgesehen. Der Kennwert-Speicherteil 25 ist zum Speichern eines Kennwertes CV vorgesehen. Die Speichermittel 23 weisen einen Versorgungseingang 26

auf, über den den Speichermitteln 23 die Versorgungsspannung V zuführbar ist. Mit den Speichermitteln 23 ist eine fünfte BUS-Verbindung 27 verbunden, die andererseits mit den zweiten Datenverarbeitungsmitteln 17 verbunden ist. Über die fünfte BUS-Verbindung 27 ist ein bidirektionales Übertragen von Daten zwischen den zweiten Datenverarbeitungsmitteln 17 und den Speichermitteln 23 und ein Übertragen des Kennwertes CV von den Speichermitteln 23 zu den zweiten Datenverarbeitungsmitteln 17 möglich. Wie dies in der Figur 1 mit strichlierten Linien angedeutet ist, kann zwischen dem Kennwert-Speicherteil 25 und den zweiten Datenverarbeitungsmitteln 17 eine separate BUS- Verbindung 28 vorgesehen sein, über die ein Austausch von mindestens einem Kennwert CV zwischen dem Kennwert-Speicherteil 25 und den zweiten Datenverarbeitungsmitteln 17 möglich ist.

Mit den zweiten Datenverarbeitungsmitteln 17 sind den zweiten Datenverarbeitungsmitteln 17 über die zweite BUS-Verbindung 16 von den ersten Datenverarbeitungsmittel 11 her zugeführte Daten DA verschlüsselbar, was im Zuge eines Verschlüsselungsvorganges durchgeführt wird. Bei einem solchen Verschlüsselungsvorgang werden die hierbei erzeugten verschlüsselten Daten DA über die fünfte BUS-Verbindung 27 dem Datenspeicherteil 24 der Speichermittel 23 zugeführt und darin gespeichert.

Mit den zweiten Datenverarbeitungsmitteln 17 sind den zweiten Datenverarbeitungsmitteln 17 über die BUS-Verbindung 27 zugeführte und aus dem Datenspeicherteil 24 der Speichermittel 23 ausgelesene Daten DA in einem weiteren Verschlüsselungsvorgang verschlüsselbar, wobei die verschlüsselten Daten DA über die zweite BUS-Verbindung 16 den ersten Datenverarbeitungsmitteln 11 zuführbar sind, in denen ein weiteres Verarbeiten der verschlüsselten Daten DA erfolgt, wobei schließlich entsprechend diesen verschlüsselten Daten DA eine Belastungsmodulation über die Verbindung 13B durchgeführt wird, was in den Empfangs/Sende-Mitteln 4 das belastungsmodulierte Trägersignal CSB zur Folge hat.

Beim Durchführen von solchen Verschlüsselungsvorgängen sorgen die Ablaufsteuermittel 15 für eine Steuerung der zweiten Datenverarbeitungsmittel 17, und zwar im wesentlichen auf die Weise, daß die Ablaufsteuermittel 15 aus dem in den Programmspeichermitteln 20 gespeicherten Programm P aufeinanderfolgend die Programmbefehle CO1, CO2 usw. über die vierte BUS-Verbindung 21 auslesen, wonach

dann ein dem jeweils ausgelesenen Programmbefehl entsprechender Verarbeitungsschritt in den zweiten Datenverarbeitungsmitteln 17 durchgeführt wird. Bei einem solchen Verarbeiten von Daten DA mit den zweiten Datenverarbeitungsmitteln 17 unter der dem in den Programmspeichermitteln 20 gespeicherten Programm P entsprechenden Steuerung mit Hilfe der Ablaufsteuermittel 15 tritt als Folge der Datenverarbeitung im Bereich der Leitungskonfiguration 3 ein Stromspitzenmuster auf. Hierbei ist die Musterkonfiguration des Stromspitzenmusters von den Programmbefehlen CO1, CO2 usw. bis COR und von den verarbeiteten Daten DA und von dem Kennwert CV abhängig.

Bei dem Datenträger 1 bzw. der Schaltung 2 ist vorteilhafterweise die Ausbildung so getroffen, daß die Schaltung 2 zusätzlich Reihenfolge-Festlegungsmittel 29 enthält, die mit den Ablaufsteuermitteln 15 zusammenwirken und mit denen bei jedem Abarbeiten des Algorithmus, der durch das in den Programmspeichermitteln 20 gespeicherte Programm gebildet ist, aus einer Vielzahl von möglichen Reihenfolgen für das Abarbeiten der N Teilalgorithmen, also der N Programmblöcke PB1, PB2 usw. bis PBN, eine Reihenfolge festlegbar ist.

Die Reihenfolge-Festlegungsmittel 29 weisen im vorliegenden Fall einen Zufallszahlengenerator 30 auf. Der Zufallszahlengenerator 30 ist mit einem Versorgungseingang 31 versehen, über den dem Zufallszahlengenerator 30 die Versorgungsspannung V zuführbar ist. Der Zufallszahlengenerator 30 ist über eine sechste BUS-Verbindung 32 mit den Ablaufsteuermitteln 15 verbunden. Auf diese Weise ist jede mit dem Zufallszahlengenerator 30 erzeugte Zufallszahl Z über die sechste BUS-Verbindung 32 den Ablaufsteuermitteln 15 zuführbar. Mit den Reihenfolge-Festlegungsmitteln 29, die den Zufallszahlengenerator 30 enthalten, ist bei jedem Abarbeiten des in den Programmspeichermitteln 20 gespeicherten Programmes P eine durch eine mit dem Zufallszahlengenerator 30 erzeugte Zufallszahl Z bestimmte Reihenfolge für das Abarbeiten der N Programmblöcke PB1 bis PBN des Programmes P festlegbar.

Hierfür weisen die Reihenfolge-Festlegungsmittel 29 zusätzlich Reihenfolge-Auswahlmittel 33 auf, die in den Ablaufsteuermitteln 15 enthalten sind. In den Reihenfolge-Auswahlmitteln 33 sind mögliche Reihenfolgen für das Abarbeiten der N Programmblöcke PB1 bis PBN des Programmes P enthalten. Vorzugsweise sind in den Reihenfolge-Auswahlmitteln 33 von sämtlichen möglichen Reihenfolgen nur ein Teil

dieser Reihenfolgen enthalten. Die Reihenfolge-Auswahlmittel 33 wirken mit dem Zufallszahlengenerator 30 zusammen, und zwar in der Weise, daß mit den Reihenfolge-Auswahlmitteln 33 entsprechend einer ihnen von dem Zufallszahlengenerator 30 über die sechste BUS-Verbindung 32 her zugeführten Zufallszahl Z aus den in den Reihenfolge-Auswahlmitteln 33 enthaltenen möglichen Reihenfolgen eine Reihenfolge auswählbar ist.

Die ersten Datenverarbeitungsmittel 11 und die Ablaufsteuermittel 15 und die zweiten Datenverarbeitungsmittel 17 und die Programmspeichermittel 20 und die Speichermittel 23 und der Zufallsgenerator 30 bilden je einen Schaltungsteil der Schaltung 2, welche Schaltungsteile über die Leitungskonfiguration 3 mit der Versorgungsspannung V versorgbar sind.

Im folgenden ist die Funktionsweise des Datenträgers 1 bzw. der Schaltung 2 im Hinblick auf das Verarbeiten von Daten DA mit den zweiten Datenverarbeitungsmitteln 17 unter der dem Programm P entsprechenden Steuerung mit Hilfe der Ablaufsteuermittel 15 beschrieben, wobei die Darstellung der Programmblöcke PB1 bis PBN in der Figur 2 zu Hilfe genommen wird.

Es sei angenommen, daß im Zuge eines Datenverarbeitungsvorganges in dem Datenträger 1 bzw. mit der Schaltung 2 des Datenträgers 1 die zweiten Datenverarbeitungsmittel 17, die zum Verarbeiten von Daten DA unter Verwendung des Kennwertes CV ausgebildet sind, aufeinanderfolgend für drei Datenverarbeitungszyklen aktiviert werden, die in der Figur 2 mit RUN1, RUN2 und RUN3 bezeichnet sind. Bevor im Zuge eines solchen Datenverarbeitungsvorganges der erste Datenverarbeitungszyklus RUN1 der zweiten Datenverarbeitungsmittel 17 erreicht wird, wird auf nicht näher beschriebene Weise der Zufallszahlengenerator 30 aktiviert, wonach der Zufallszahlengenerator 30 eine Zufallszahl Z1 erzeugt und über die sechste BUS-Verbindung 32 den Reihenfolge-Auswahlmitteln 33 zuführt. Die Reihenfolge-Auswahlmittel 33 wählen dann entsprechend der ihnen von dem Zufallszahlengenerator 30 her zugeführten Zufallszahl Z1 eine Reihenfolge für das Abarbeiten der N Programmblöcke PB1 bis PBN des Programmes P aus, beispielsweise die in der linken Spalte gemäß der Figur 2 angegebene Reihenfolge PB1, PB2, PB4, PB6, PB3, ... PB5 und PBN. Im Anschluß daran werden die Programmblöcke PB1 bis PBN in der vorstehend angeführten Reihenfolge abgearbeitet. Hierbei werden alle in den vorgenannten Programmblöcken enthaltenen Programmbefehle CO1, CO2, ... COR, CO1, CO2, ...

COR usw. bis CO1, CO2 ..... COR abgearbeitet, was bedeutet, daß die aufeinanderfolgenden Programmbefehle CO1, CO2 bis COR insgesamt N-mal aufeinanderfolgend abgearbeitet werden, wie dies in der rechten Spalte der Figur 2 angegeben ist.

Wenn bei dem Datenverarbeitungsvorgang der zweite Datenverarbeitungszyklus RUN2 abgearbeitet werden soll, wird zuvor wiederum der Zufallszahlengenerator 30 aktiviert, was zur Folge hat, daß der Zufallszahlengenerator 30 eine zweite Zufallszahl Z2 abgibt. Die zweite Zufallszahl Z2 wird über die sechste BUS-Verbindung 32 den Reihenfolge-Auswahlmitteln 33 zugeführt, was zur Folge hat, daß die Reihenfolge-Auswahlmittel eine weitere Reihenfolge auswählt, beispielsweise die in der zweiten Spalte der Figur 2 angegebene Reihenfolge PB6, PB3, PB7, PBN, PB1, ... PB4 und PB2. Somit liegt beim zweiten Datenverarbeitungszyklus RUN2 eine gänzlich andere Reihenfolge für das Abarbeiten der N Programmblöcke vor. Die Reihenfolge der Programmbefehle CO1, CO2 bis COR usw. bleibt jedoch unverändert.

Wenn im Zuge des angenommenen Datenverarbeitungsvorganges der dritte Datenverarbeitungszyklus RUN3 abzuarbeiten ist, wird analog wie bereits zuvor beschrieben, der Zufallszahlengenerator 30 neuerlich aktiviert, so daß derselbe die Zufallszahl Z3 erzeugt und über die sechste BUS-Verbindung 32 den Ablaufsteuermitteln 15 bzw. den darin enthaltenen Reihenfolge-Auswahlmitteln 33 zuführt. Dies hat zur Folge, daß die Reihenfolge-Auswahlmittel 33 eine weitere Reihenfolge für das Abarbeiten der N Programmblöcke PB1 bis PBN auswählen, nämlich beispielsweise die in der dritten Spalte der Figur 2 dargestellte Reihenfolge PBN, PB1, PB4, PB6, PB3, ... PB7 und PB2. Somit ist bei dem dritten Datenverarbeitungszyklus RUN3 wieder eine neue Reihenfolge für das Abarbeiten der N Programmblöcke PB1 bis PBN des Programmes P gegeben, wobei die Aufeinanderfolge der Programmbefehle CO1, CO2 bis COR usw. wiederum unverändert gleich ist.

Wie aus der vorstehenden Beschreibung klar hervorgeht, ist bei dem Datenträger 1 gemäß der Figur 1 bzw. bei der Schaltung 2 des Datenträgers 1 erreicht, daß zwar die Aufeinanderfolge aller Programmbefehle COX aus allen hintereinander abgearbeiteten Programmblöcken PBX bei jedem Abarbeiten des Programmes P stets gleich ist, daß aber die Reihenfolge für das Abarbeiten der N Programmblöcke PBX des Programmes P bei jedem Abarbeiten dieses Programmes P unterschiedlich ist. Hierdurch ist erreicht, daß die

Reihenfolge des Abarbeitens der N Programmblöcke PBX von außerhalb des Datenträgers 1 bzw. der Schaltung 2 des Datenträgers 1 nicht ermittelt werden können. Dadurch ist es auch nicht möglich, aufeinanderfolgend verursachte Reihenfolgen von Stromspitzenmustern, die durch aufeinanderfolgendes Aktivieren des Programmes P verursacht werden, untereinander zu vergleichen und für Analysemethoden mit Hilfe von Korrelationsverfahren bzw. und damit die Reihenfolge des Auftretens der N Stromspitzenmuster, von denen jedes beim Abarbeiten eines Programmblockes PBX entsteht, Vergleichsverfahren zu verwenden. Hierdurch ist somit erreicht, daß ein unerwünschtes Erkennen bzw. Feststellen des in den zweiten Datenverarbeitungsmitteln 17 verwendeten Kennwertes CV praktisch nicht möglich ist.

Bei einem Datenträger gemäß einem weiteren Ausführungsbeispiel, das jedoch nicht dargestellt ist, ist anstelle der Programmspeichermittel 20 eine festverdrahtete Logikschaltung vorgesehen, die mit den Ablaufsteuermitteln 15 zusammenwirkt und in der ein Algorithmus auf festverdrahtete, also hardwaremäßige Weise enthalten ist. Mit diesem auf hardwaremäßige Weise in der festverdrahteten Logikschaltung gespeicherten Algorithmus ist auf analoge Weise eine Steuerung der zweiten Datenverarbeitungsmittel 17 mit Hilfe der Ablaufsteuermittel 15 ermöglicht.

Die Erfindung ist auf die Datenverarbeitungseinrichtung, also den Datenträger 1 gemäß dem anhand der Figur 1 vorstehend beschriebenen Ausführungsbeispiel nicht beschränkt. Bei dem Datenträger 1 gemäß der Figur 1 sind die Reihenfolge-Auswahlmittel 33 als Teil der Ablaufsteuermittel 15 ausgebildet, wobei die Reihenfolge-Auswahlmittel 33 hardwaremäßig realisiert sind. Bei einer anderen nicht dargestellten Ausführungsform einer erfindungsgemäßen Datenverarbeitungseinrichtung können die Reihenfolge-Auswahlmittel 33 auch mit Hilfe eines Auswahlprogrammes realisiert sein, wobei dieses Auswahlprogramm Teil des in den Programmspeichermitteln 20 gespeicherten Programmes P ist. In diesem Fall wirkt dann der Zufallszahlengenerator 30 über eine BUS-Verbindung mit den zweiten Datenverarbeitungsmitteln 17 unmittelbar zusammen. Es sei weiters noch erwähnt, daß bei dem Datenträger 1 gemäß der Figur 1 das in den Programmspeichermitteln 20 enthaltene Programm P Teil eines umfangreicheren Programmes ist. Bezüglich der Aufeinanderfolge der Programmblöcke PB1 bis PBN, wie diese in der Figur 2 dargestellt sind, sei noch erwähnt, daß die Programmblöcke nicht unmittelbar aufeinanderfolgend abgearbeitet werden müssen, sondern daß beim Abarbeiten

zwischen zwei aufeinanderfolgenden Programmblöcken PB auch ein Programmteil eines anderen Programmes abgearbeitet kann.

Patentansprüche:

1. Datenverarbeitungseinrichtung mit einer Schaltung,
die aus verschiedenen Schaltungsteilen besteht, die über eine Leitungskonfiguration mit einer Versorgungsspannung versorgbar sind, und
die Datenverarbeitungsmittel enthält, die einen solchen mit der Versorgungsspannung versorgbaren Schaltungsteil bilden und die zum Verarbeiten von Daten unter Verwendung eines Kennwertes geeignet sind, und
die Ablaufsteuermittel enthält, die auch einen solchen mit der Versorgungsspannung versorgbaren Schaltungsteil bilden und die zum Abarbeiten eines Algorithmus zum Steuern der Datenverarbeitungsmittel entsprechend diesem Algorithmus ausgebildet sind, welcher Algorithmus eine bestimmte Anzahl N von Teilalgorithmen umfaßt, in denen identische Aufeinanderfolgen von Algorithmusschritten enthalten sind und die bei jedem Abarbeiten des Algorithmus in einer bestimmten Reihenfolge abarbeitbar sind, und
bei der - bei einem Verarbeiten von Daten mit den Datenverarbeitungsmitteln unter der dem Algorithmus entsprechenden Steuerung mit Hilfe der Ablaufsteuermittel - als Folge der Datenverarbeitung im Bereich der Leitungskonfiguration ein Stromspitzenmuster auftritt, wobei die Musterkonfiguration des Stromspitzenmusters von den Algorithmusschritten und von den verarbeiteten Daten und von dem Kennwert abhängig ist,
dadurch gekennzeichnet,
daß die Schaltung zusätzlich Reihenfolge-Festlegungsmittel enthält, die mit den Ablaufsteuermitteln zusammenwirken und mit denen bei jedem Abarbeiten des Algorithmus aus einer Vielzahl von möglichen Reihenfolgen für das Abarbeiten der N Teilalgorithmen eine Reihenfolge festlegbar ist.

2. Datenverarbeitungseinrichtung nach Anspruch 1, dadurch gekennzeichnet,
daß die Reihenfolge-Festlegungsmittel einen Zufallszahlengenerator aufweisen und
daß mit den bei jedem Abarbeiten des Algorithmus eine durch eine mit dem Zufallszahlengenerator erzeugte Zufallszahl bestimmte Reihenfolge für das Abarbeiten der N Teilalgorithmen festlegbar ist.

3. Datenverarbeitungseinrichtung nach Anspruch 2, dadurch gekennzeichnet,
daß die Reihenfolge-Festlegungsmittel zusätzlich Reihenfolge-Auswahlmittel aufweisen, in denen mögliche Reihenfolgen für das Abarbeiten der N Teilalgorithmen enthalten sind

und die mit dem Zufallszahlengenerator zusammenwirken, und
daß mit den Reihenfolge-Auswahlmitteln entsprechend einer ihnen von dem Zufallszahlengenerator her zugeführten Zufallszahl aus den möglichen Reihenfolgen eine Reihenfolge auswählbar ist.

4. Datenverarbeitungseinrichtung nach Anspruch 1, dadurch gekennzeichnet, daß Speichermittel vorgesehen sind, die mit den Ablaufsteuermitteln zusammenwirken und in denen der Algorithmus in Form eines Programmes gespeichert ist, das als Teilalgorithmen N Programmblöcke umfaßt, in denen als Algorithmusschritte Programmbefehle enthalten sind.

5. Datenverarbeitungseinrichtung nach Anspruch 1, dadurch gekennzeichnet, daß eine festverdrahtete Logikschaltung vorgesehen ist, die mit den Ablaufsteuermitteln zusammenwirkt und in der der Algorithmus auf festverdrahtete, also hardwaremäßige Weise enthalten ist.

6. Datenverarbeitungseinrichtung nach Anspruch 1, dadurch gekennzeichnet, daß die Datenverarbeitungsmittel durch Mittel zum Verschlüsseln und/oder Entschlüsseln von Daten gebildet sind.

7. Datenverarbeitungseinrichtung nach Anspruch 1, dadurch gekennzeichnet, daß die Datenverarbeitungseinrichtung durch einen Datenträger gebildet ist, dessen Schaltung in integrierter Technik realisiert ist.

8. Schaltung für eine Datenverarbeitungseinrichtung,
die aus verschiedenen Schaltungsteilen besteht, die über eine Leitungskonfiguration mit einer Versorgungsspannung versorgbar sind, und
die Datenverarbeitungsmittel enthält, die einen solchen mit der Versorgungsspannung versorgbaren Schaltungsteil bilden und die zum Verarbeiten von Daten unter Verwendung eines Kennwertes geeignet sind, und
die Ablaufsteuermittel enthält, die auch einen solchen mit der Versorgungsspannung versorgbaren Schaltungsteil bilden und die zum Abarbeiten eines Algorithmus zum Steuern der Datenverarbeitungsmittel entsprechend diesem Algorithmus ausgebildet sind, welcher Algorithmus eine bestimmte Anzahl N von Teilalgorithmen umfaßt, in denen identische Aufeinanderfolgen von Algorithmusschritten enthalten sind und die bei jedem Abarbeiten des Algorithmus in einer bestimmten Reihenfolge abarbeitbar sind, und
bei der - bei einem Verarbeiten von Daten mit den Datenverarbeitungsmitteln unter der

dem Algorithmus entsprechenden Steuerung mit Hilfe der Ablaufsteuermittel - als Folge der Datenverarbeitung im Bereich der Leitungskonfiguration ein Stromspitzenmuster auftritt, wobei die Musterkonfiguration des Stromspitzenmusters von den Algorithmusschritten und von den verarbeiteten Daten und von dem Kennwert abhängig ist,

dadurch gekennzeichnet,

daß die Schaltung zusätzlich Reihenfolge-Festlegungsmittel enthält, die mit den Ablaufsteuermitteln zusammenwirken und mit denen bei jedem Abarbeiten des Algorithmus aus einer Vielzahl von möglichen Reihenfolgen für das Abarbeiten der N Teilalgorithmen eine Reihenfolge festlegbar ist.

9. Schaltung nach Anspruch 8, dadurch gekennzeichnet,

daß die Reihenfolge-Festlegungsmittel einen Zufallszahlengenerator aufweisen und daß mit den bei jedem Abarbeiten des Algorithmus eine durch eine mit dem Zufallszahlengenerator erzeugte Zufallszahl bestimmte Reihenfolge für das Abarbeiten der N Teilalgorithmen festlegbar ist.

10. Schaltung nach Anspruch 9, dadurch gekennzeichnet,

daß die Reihenfolge-Festlegungsmittel zusätzlich Reihenfolge-Auswahlmittel aufweisen, in denen mögliche Reihenfolgen für das Abarbeiten der N Teilalgorithmen enthalten sind und die mit dem Zufallszahlengenerator zusammenwirken, und

daß mit den Reihenfolge-Auswahlmitteln entsprechend einer ihnen von dem Zufallszahlengenerator her zugeführten Zufallszahl aus den möglichen Reihenfolgen eine Reihenfolge auswählbar ist.

11. Schaltung nach Anspruch 8, dadurch gekennzeichnet,

daß Speichermittel vorgesehen sind, die mit den Ablaufsteuermitteln zusammenwirken und in denen der Algorithmus in Form eines Programmes gespeichert ist, das als Teilalgorithmen N Programmblöcke umfaßt, in denen als Algorithmusschritte Programmbefehle enthalten sind.

12. Schaltung nach Anspruch 8, dadurch gekennzeichnet,

daß eine festverdrahtete Logikschaltung vorgesehen ist, die mit den Ablaufsteuermitteln zusammenwirkt und in der der Algorithmus auf festverdrahtete, also hardwaremäßige Weise enthalten ist.

13. Schaltung nach Anspruch 8, dadurch gekennzeichnet,

daß die Datenverarbeitungsmittel durch Mittel zum Verschlüsseln und/oder Entschlüsseln von Daten gebildet sind.

14. Schaltung nach Anspruch 8, dadurch gekennzeichnet, daß die Schaltung für eine durch einen Datenträger gebildete Datenverarbeitungseinrichtung vorgesehen ist und daß die Schaltung in integrierter Technik realisiert ist.

Zusammenfassung

Datenverarbeitungseinrichtung mit einen Kennwert nutzenden Datenverarbeitungsmitteln und mit Mitteln zum Abwehren von Analysemethoden zur Ermittlung des Kennwertes

Bei einer Datenverarbeitungseinrichtung (1) mit einer Schaltung (2), die Datenverarbeitungsmittel (17) enthält, die zum Verarbeiten von Daten (DA) unter Verwendung eines Kennwertes (CV) geeignet sind, und die Ablaufsteuermittel (15) enthält, die zum Abarbeiten eines Algorithmus zum Steuern der Datenverarbeitungsmittel (17) entsprechend diesem Algorithmus ausgebildet sind, wobei der Algorithmus eine bestimmte Anzahl N von Teilalgorithmen umfaßt, in denen identische Aufeinanderfolgen von Algorithmusschritten enthalten sind, sind zusätzlich Reihenfolge-Festlegungsmittel (29) vorgesehen, die mit den Ablaufsteuermitteln (15) zusammenwirken und mit denen bei jedem Abarbeiten des Algorithmus aus einer Vielzahl von möglichen Reihenfolgen für das Abarbeiten der N Teilalgorithmen eine Reihenfolge festlegbar ist.

(Figur 1).

1/2

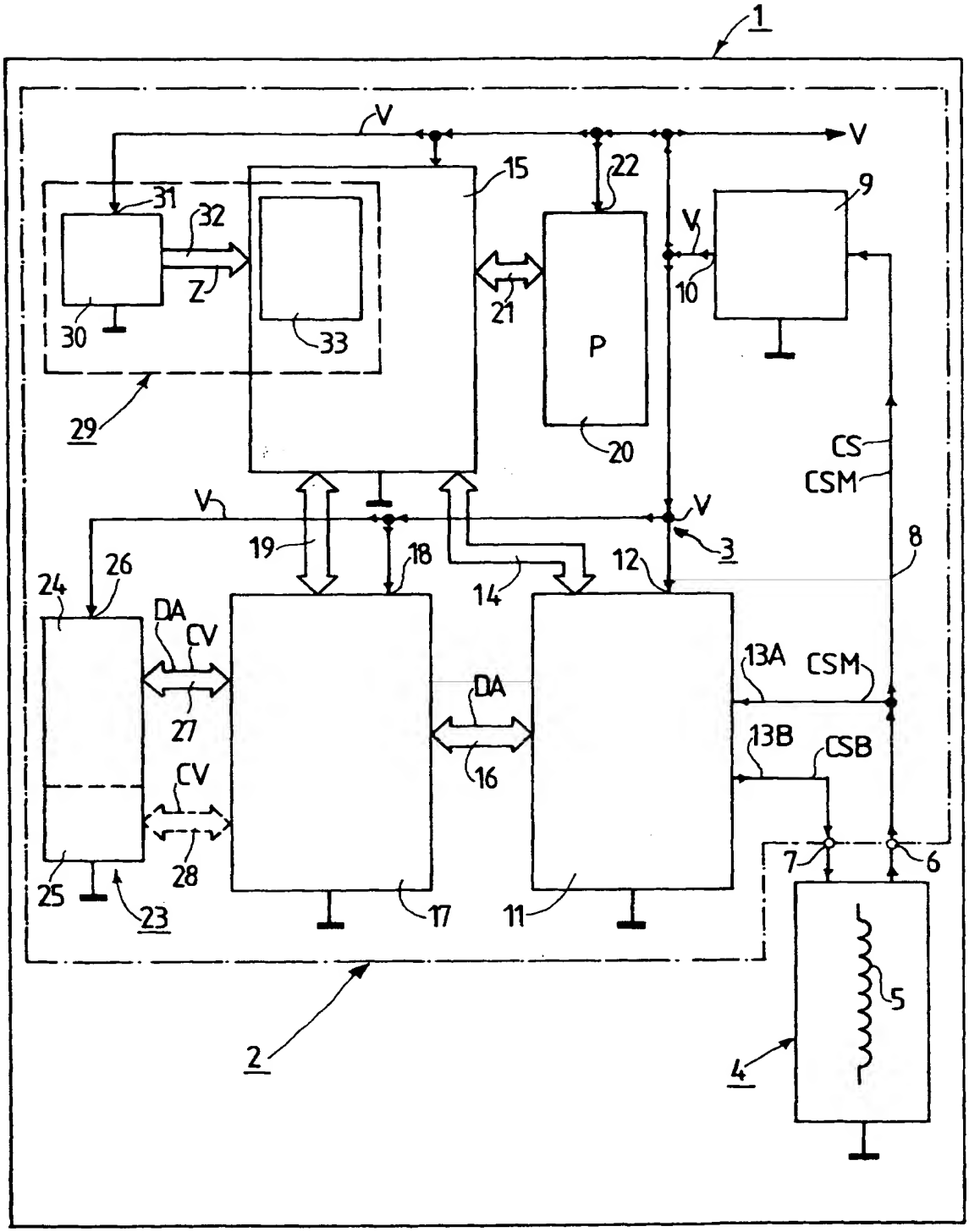
1
V
V
15
22
9
31
32
Z
V
10
30
33
21
P
29
20
CS
CSM
V
V
19
18
12
3
8
24
26
14
DA
CV
13A
CSM
27
DA
16
13B
CSB
CV
28
7
6
25
23
17
11
5
2
4

FIG.1

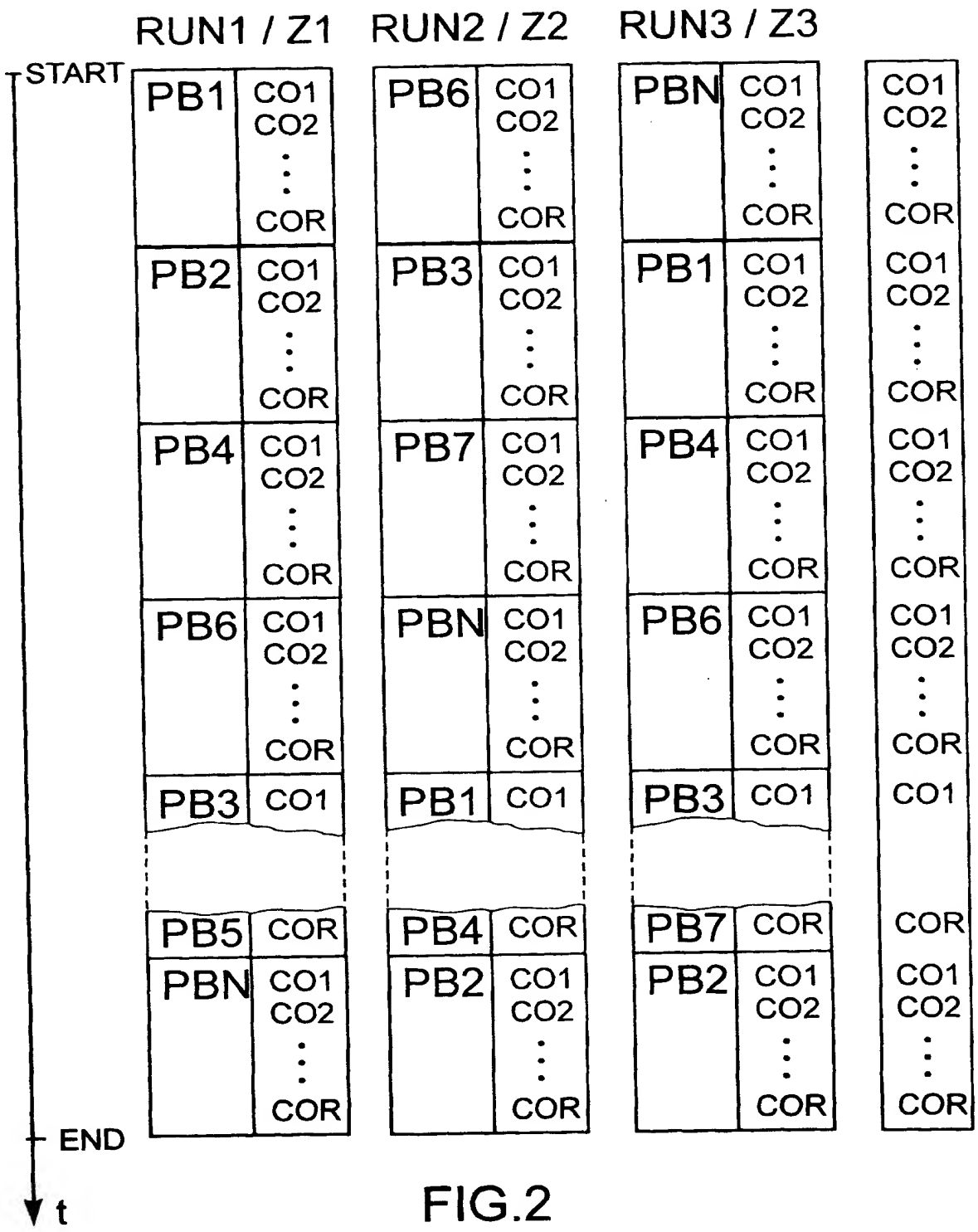
RUN1 / Z1
RUN2 / Z2
RUN3 / Z3
START
END
t
PB1
PB2
PB4
PB6
PB3
PB5
PBN
PB6
PB3
PB7
PBN
PB1
PB4
PB2
PBN
PB1
PB4
PB6
PB3
PB7
PB2
CO1
CO2
COR

FIG.2